Internal Pentest

Executive Summary

Sample Internal Pentest
H3 Sample Account
May 24, 2024

HORIZON3.ai
~~TRUST~~ BUT VERIFY

Website	**https://www.horizon3.ai**
Email	**info@horizon3.ai**
Twitter	**@Horizon3ai**
LinkedIn	**Horizon3.ai**

Summary

Started	**May 24, 2024, 9:08 PM UTC**	Initiated by	**Horizon 3 AI**	NodeZero IP	**10.0.227.200**
Completed	**May 24, 2024, 9:43 PM UTC**	For client	**H3 Sample Account**	Hosts Assessed	**118**
Duration	**34m**				

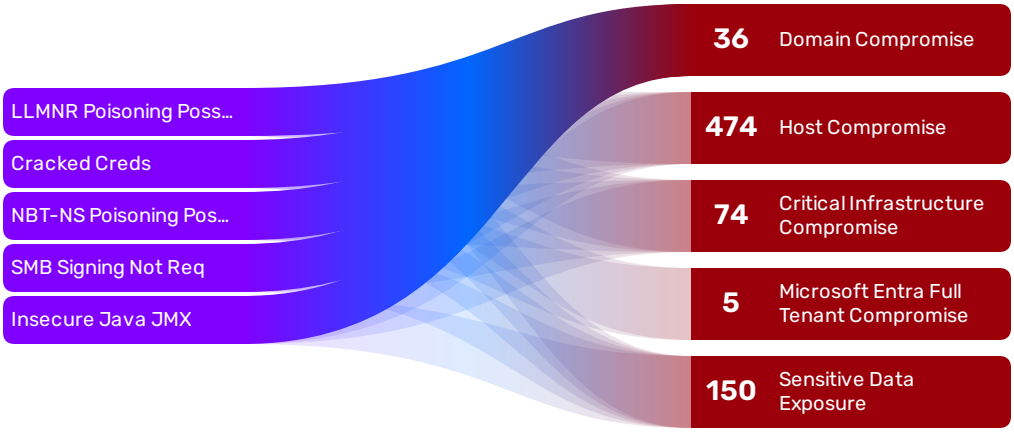
895	716	723	1K	84
Attack Paths Exploited	**Weaknesses Found**	**Credentials Compromised**	**Protected Data Items**	**Hosts Compromised**

Overall Exposure Level: Critical

This exposure level stems from finding and exploiting **critical weaknesses** in the network, leading to **Domain Compromise, Business Email Compromise, and AWS User/Role Compromise**. 84 hosts, or **71% of hosts** in scope, were compromised.

To reduce the exposure level, remediate the weaknesses that led to the greatest impacts and compromised hosts. To further improve cyber resilience, implement the security policy recommendations provided to address any systemic issues affecting the environment as a whole.

Top Impacts

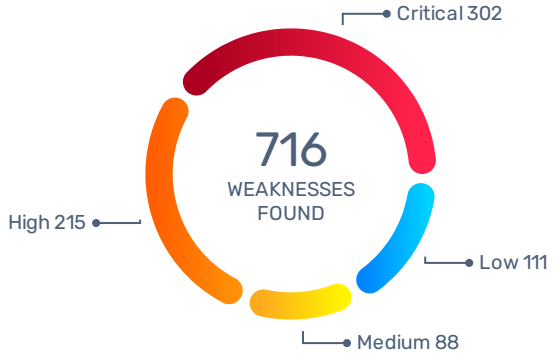


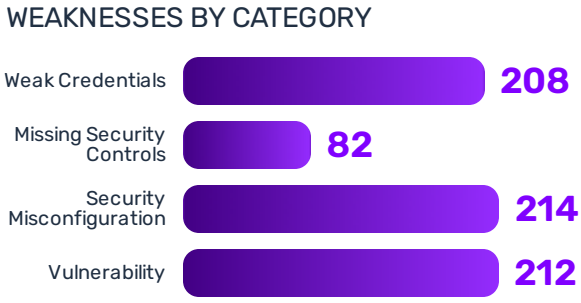
Once a domain is fully compromised, all hosts, domain user accounts, data, infrastructure and applications tied to that domain should be considered fully compromised. Additionally, applications running on a domain-joined machine or any application that uses Active Directory integration to authenticate users should be considered fully compromised.

Top impacts found along the 895 attack paths exploited during the pentest:

1. **Domain Compromise**: Compromised the domain administrator accounts for administrator, Administrator, a-jsmith, and cbr-user in domain POD04.EXAMPLE.INTERNAL. These accounts have unlimited access within the domain and can perform sensitive actions such as reading all employee email, accessing business data, or disabling the entire company's access to the network.
2. **Domain Compromise**: Compromised the domain administrator accounts for admin1, administrator, and 5 other accounts in domain SMOKE.NET. These accounts have unlimited access within the domain and can perform sensitive actions such as reading all employee email, accessing business data, or disabling the entire company's access to the network.
3. **Domain Compromise**: Discovered and exploited critical vulnerabilities affecting domain controller 10.0.4.1 (dc01.pod04.example.internal) and domain controller 10.0.4.2 (dc02.pod04.example.internal) in domain POD04.EXAMPLE.INTERNAL. Domain controllers are highly privileged machines that control identity and access management for the entire organization. By compromising the domain controller, NodeZero effectively gained unrestricted access to all hosts, credentials, and business data in the organization connected to the domain.

Top Weaknesses





Fix the weaknesses from the most impactful weakness types found during the pentest:

1. **H3-2021-0034: LLMNR Poisoning Possible** affecting host 10.0.227.51 and 234 other hosts. A captured hash credential can be cracked offline to discover the plaintext password for reuse on other systems or the hash can be relayed and used to access other systems as well. Likewise, a captured plaintext credential can be immediately used to access other systems. The weakness was leveraged in **235 attack paths** leading to **Domain Compromise, Ransomware Exposure, and 7 other impacts**.
2. **H3-2021-0020: Cracked Creds** affecting a cleartext password for it_support and 195 other credentials. An attacker can openly maneuver throughout an environment and access information if a password is compromised. The weakness was leveraged in **193 attack paths** leading to **Domain Compromise, Microsoft Entra Full Tenant Compromise, and 6 other impacts**.
3. **H3-2021-0035: NBT-NS Poisoning Possible** affecting host 10.0.227.51 and 165 other hosts. A captured hash credential can be cracked offline to discover the plaintext password and also be relayed for reuse on other systems. Likewise, a captured plaintext credential can be immediately used to access other systems. The weakness was leveraged in **166 attack paths** leading to **Domain Compromise, Microsoft Entra Full Tenant Compromise, and 6 other impacts**.

Systemic Issues

Issue	Policy Recommendation
Credential Reuse **21** Hosts that NodeZero compromised by reusing local administrator passwords	**Implement LAPS** Microsoft's Local Administrator Password Solution (LAPS) centralizes management of local admin passwords in Active Directory for all domain-joined machines. LAPS ensures all local admin passwords are unique and random, eliminating this form of credential reuse as an attack vector.
Critical Vulnerabilities **48** Hosts that NodeZero compromised via CISA known exploited vulnerabilities, including domain controllers and VMware vCenter servers	**Improve Vulnerability Management** Known exploited vulnerabilities should be patched or mitigated in an efficient manner to make it harder for attackers to achieve initial access or move laterally through an environment.
Unmanaged Data **406K** Files that NodeZero found to be accessible to anonymous users	**Classify and Protect Data** Data in large network file shares should be classified based on sensitivity and restricted to users on a least-privilege basis.

NodeZero identified important systemic issues affecting the overall environment. Addressing these issues will improve the environment's resilience to future cyber attacks.

1. **Credential Reuse**: NodeZero compromised 21 hosts by reusing local administrator passwords. Microsoft's Local Administrator Password Solution (LAPS) centralizes management of local admin passwords in Active Directory for all domain-joined machines. LAPS ensures all local admin passwords are unique and random, eliminating this form of credential reuse as an attack vector.
2. **Critical Vulnerabilities**: NodeZero compromised 48 hosts via CISA known exploited vulnerabilities, including domain controllers and VMware vCenter servers. Known exploited vulnerabilities should be patched or mitigated in an efficient manner to make it harder for attackers to achieve initial access or move laterally through an environment.
3. **Unmanaged Data**: NodeZero found 405,804 files to be accessible to anonymous users. Data in large network file shares should be classified based on sensitivity and restricted to users on a least-privilege basis.

MITRE

This diagram illustrates the actions of NodeZero, as they pertain to MITRE tactics and techniques. Each tile indicates how many attack modules were used for a given technique during the pentest. A total of **29,763 attack modules** employed **72 techniques** across **13 MITRE tactics**.

Reconnaissance

Gather Victim Host Information 1K T1592	Gather Victim Network Information 696 T1590	Active Scanning 670 T1595	Search Victim-Owned Websites 560 T1594	Search Open Technical Databases 19 T1596
Gather Victim Identity Information 15 T1589	Search Open Websites / Domains 3 T1593			

Resource Development

Compromise Infrastructure 15 T1584				

Initial Access

Valid Accounts 3.8K T1078	Exploit Public-Facing Application 581 T1190	External Remote Services 116 T1133		

Execution

Command and Scripting Interpreter 356 T1059	Scheduled Task / Job 35 T1053	Windows Management Instrumentation 34 T1047	System Services 34 T1569	Exploitation for Client Execution 1 T1203

Persistence

Account Manipulation	13	T1098
Create Account	2	T1136

Privilege Escalation

Exploitation for Privilege Escalation	68	T1068
Abuse Elevation Control Mechanism	16	T1548
Valid Accounts	11	T1078
Access Token Manipulation	1	T1134

Defense Evasion

Indicator Removal on Host	23	T1070

Credential Access

Unsecured Credentials	5.6K	T1552
Brute Force	1.2K	T1110
OS Credential Dumping	340	T1003
Exploitation for Credential Access	187	T1212
Credentials from Password Stores	116	T1555
Steal or Forge Kerberos Tickets	41	T1558
Forced Authentication	13	T1187
Steal Application Access Token	6	T1528
Adversary-in-the-Middle	1	T1557

Discovery

Network Service Scanning	1.4K	T1046
Software Discovery	701	T1518
Account Discovery	576	T1087
Permission Groups Discovery	554	T1069
Remote System Discovery	537	T1018
System Information Discovery	411	T1082
Cloud Infrastructure Discovery	173	T1580
Network Share Discovery	150	T1135
File and Directory Discovery	143	T1083
Cloud Service Discovery	127	T1526
System Owner / User Discovery	113	T1033
System Service Discovery	90	T1007
Container and Resource Discovery	53	T1613
Process Discovery	42	T1057
Domain Trust Discovery	32	T1482
Group Policy Discovery	32	T1615
System Network Configuration Discovery	22	T1016
Password Policy Discovery	5	T1201
System Network Connections Discovery	4	T1049
Cloud Storage Object Discovery	1	T1619

Lateral Movement

Remote Services 3.1K T1021	Use Alternate Authentication Material 1.1K T1550	Exploitation of Remote Services 608 T1210	Lateral Tool Transfer 248 T1570

Collection

Data from Network Shared Drive 1.5K T1039	Screen Capture 425 T1113	Data from Cloud Storage Object 371 T1530	Data from Local System 69 T1005	Automated Collection 41 T1119
Data from Information Repositories 39 T1213	Archive Collected Data 32 T1560	Data from Configuration Repository 6 T1602	Email Collection 3 T1114	Adversary-in-the-Middle 1 T1557

Command and Control

Application Layer Protocol 567 T1071	Non-Application Layer Protocol 328 T1095	Encrypted Channel 249 T1573	Non-Standard Port 249 T1571

Impact

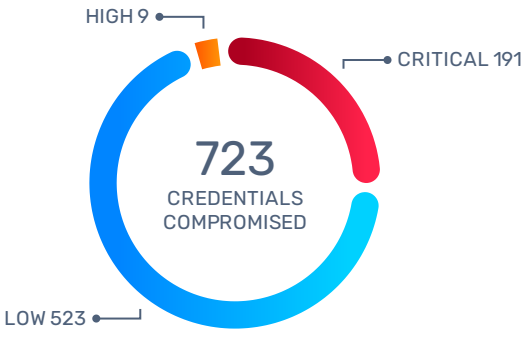
Data Manipulation 36 T1565	Account Access Removal 1 T1531

Top Credentials

10 CRITICAL — **cbr-user@10.0.4.129:445 10.0.4.130:445 10.0.4...**
DOMAIN ADMIN

10 CRITICAL — **jsmith@10.0.220.52:445 10.0.220.53:445 10.0....**
DOMAIN USER

10 CRITICAL — **it_support**



As illustrated by severity, the pentest discovered **723 credentials** in total, with **191 CRITICAL credentials**. The most impactful credentials likely contribute to the most critical attack paths.